PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of

Akiko KAWAMOTO

Docket No: Q63597

Appln. No.: 09/805,116

Group Art Unit: 2135

Confirmation No.: 1497

Examiner: Thanhnga B. Truong

Filed: March 14, 2001

For: MULTICAST SYSTEM, AUTHENTICATION SERVER TERMINAL, MULTICAST □RECEIVER TERMINAL CONTROLLING METHOD, AND STORAGE MEDIUM

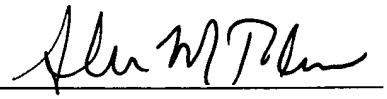
SUBMISSION OF APPEAL BRIEF

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith please find an Appeal Brief. A check for the statutory fee of $500.00 is attached. The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account. A duplicate copy of this paper is attached.

Respectfully submitted,



Allison M. Tulino
Registration No. 48,294

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: December 20, 2005

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of

Akiko KAWAMOTO

Docket No: Q63597

Appln. No.: 09/805,116

Group Art Unit: 2135

Confirmation No.: 1497

Examiner: Thanhnga B. Truong

Filed: March 14, 2001

For: MULTICAST SYSTEM, AUTHENTICATION SERVER TERMINAL, MULTICAST RECEIVER TERMINAL CONTROLLING METHOD, AND STORAGE MEDIUM

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 41.37, Appellant submits the following:

Table of Contents

I. REAL PARTY IN INTEREST

The real party in interest is NEC CORPORATION by virtue of an assignment executed by Akiko Kawamoto (hereinafter "Appellant") on February 15, 2001 and recorded in the U.S. Patent and Trademark Office on March 14, 2001 at reel 011605 and frame 0058.

II. RELATED APPEALS AND INTERFERENCES

Upon information and belief, there are no other prior or pending appeals, interferences, or judicial proceedings known to Appellant's Representative or the Assignee that my be related to, be directly affected by, or have a bearing on the Board's decision in the Appeal.

III. STATUS OF CLAIMS

Claims 1-4 and 6-11 are pending and are the basis of this Appeal (*see* Claims Appendix).

Claims 1-4 and 6-11 stand rejected.

IV. STATUS OF AMENDMENTS

Appellant did not amend the claims subsequent to the April 20, 2005 Final Office Action. Accordingly, all amendments, which have been made during prosecution of the present application, have been entered, and are reflected in the attached Claims Appendix.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The present invention is a multicast system for data communication using an authentication server. The features of independent claims 1 and 7-9 are described herein in reference to non-limiting embodiments in Appellant's specification.

Claim 1 - Claim 1 recites a multicast system having a sender terminal 110 for transmitting multicast data, a receiver terminal 130, 140 for receiving multicast data, and an authentication server processor 100 for managing the sender terminal and the receiver terminal (Figure 1). A first user processor 112 is provided in the sender terminal 110 for transmitting a login requirement to the authentication server processor 100. A second user processor 132, 142 is provided in the receiver terminal 130, 140 for transmitting a login requirement to the authentication server processor 100 (Figure 1). The authentication server processor 100 executes a logout when the second user processor 132, 142 in the receiver terminal 130, 140 does not receive a periodically distributed encryption key, where the encryption key which is periodically generated by the authentication server processor 100 and distributed to the receiver terminal (non-limiting embodiment pg. 9, line 14 to page 11, line 11).

Claim 7 - Claim 7 recites an authentication server terminal 100 having an authentication server processor 101 (Figure 1). Also, a first receiving section 200 receives a login requirement transmitted from a first user processor 112 provided in a sender terminal 110 that transmits multicast data (non-limiting embodiment page 9, lines 14-16). A second receiving section 200

receives a login requirement transmitted from a second user processor 132, 142 provided in a receiver terminal 130, 140 that receives multicast data. A user registration information section registers user's individual information 240. The sender terminal 110, which is permitted login by the authentication server processor 100, encrypts multicast data and transmits encrypted multicast data. The receiver terminal 130, 140, which is registered as a user in the user registration information section 240 by the authentication server processor 100, is permitted login and receives multicast data. The authentication server processor 100 executes a logout when the second user processor 132, 142 in the receiver terminal 130, 140 does not receive a periodically distributed encryption key which is periodically generated by the authentication server processor 100 and distributed to the receiver terminal 130, 140 (non-limiting embodiment pg. 9, line 14 to page 11, line 11).

Claim 8 - Claim 8 recites a multicast receiver terminal management method where a user's individual information transmitted from a sender terminal 110 is registered (non-limiting embodiment page 9, lines 2-13). A login requirement transmitted from the sender terminal 110, which transmits multicast data, is received (non-limiting embodiment page 9, lines 14-16). The sender terminal 110, which is permitted login so as to encrypt multicast data and to transmit encrypted multicast data, is managed. A login requirement transmitted from a receiver terminal 130, 140 which receives multicast data is received (non-limiting embodiment page 10, lines 3-8). The receiver terminal 130, 140, which is registered as a user in a user registration information section by an authentication server processor 100, so as to be permitted login and to receive

multicast data, is managed. Further, a logout is executed when the receiver terminal does not receive a periodically distributed encryption key which is periodically generated and distributed to the receiver terminal (non-limiting embodiment pg. 9, line 14 to page 11, line 11).

Claim 9 - Claim 9 recites a storage medium which is readable by a computer, for storing a multicast receiver terminal management method program for conducting multicast data communication in a computer. In a registration step, a user's individual information is registered, where the user uses a sender terminal (non-limiting embodiment page 9, lines 2-13). In a receiving step, a login requirement, transmitted from the sender terminal 110 which transmits multicast data, is received (Fig. 5). A sender terminal 110, which is permitted login, is managed so as to encrypt multicast data and to transmit encrypted multicast data (Fig. 6). In a managing step, in which a receiver terminal 130, 140, which is registered as a user in a user registration information section by an authentication server processor 100, is managed so as to be permitted to login and to receive multicast data (Fig. 6). Finally, the authentication server processor 100 executes a logout when the receiver terminal does not receive a periodically distributed encryption key which is periodically generated by the authentication server processor and distributed to the receiver terminal (non-limiting embodiment pg. 9, line 14 to page 11, line 11).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1-3 and 6-11 stand rejected under 35 U.S.C. § 103(a), as allegedly being unpatentable over U.S. Patent No. 5,748,736 to Mittra ("Mittra") in view of U.S. Patent No. 5,970,477 to Roden ("Roden").

B. Claims 1, 4 and 7-11 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent No. 6, 275, 859 to Wesley et al. ("Wesley") in view of Roden.

VII. ARGUMENT

A. Rejection of claims 1-3 and 6-11 under 35 U.S.C. § 103(a) in view of Mittra and Roden.

1. Claim 1

Appellant submits that claim 1 is patentable over the cited references. For example, claim 1 recites that the **authentication server processor executes a logout when the second user processor in the receiver terminal does not receive a periodically distributed encryption key**, which is periodically generated by the authentication server processor and distributed to the receiver terminal.

As set forth in the non-limiting embodiment on page 11 of the present Application, an encryption key encrypted using a common key is transmitted to a user. This is done on a periodic basis. The periodic transmission of the encryption key is effected in order to prevent the encryption key from being illegally obtained and used. If the key update controller (231) of the authentication server terminal receives an **acknowledgement receipt** of the key from the user, this result is stored in the server management information (250) and the process repeats. However, if the key update controller (231) **does not receive the acknowledgement receipt** of the key from the user within a predetermined time, the key update controller regards this as indicative of the fact that the user has terminated receiving keys transmitted from the authentication server terminal, causing a logout process to be executed.

Turning to the rejection, the Examiner acknowledges that Mittra fails to disclose the above feature, but contends that Roden does. In particular, the Examiner maintains that column 17, lines 35-39 of Roden discloses the above feature (pg. 4 of April 20, 2005 Final Office Action). The cited portion of Roden discusses figure 6, which is a flow diagram illustrating a method for allocating a cost associated with Internet access regarding sites accessed by an end-user (col. 17, lines 25-28). In column 17, lines 33-39, Roden teaches:

> "In decision step 604, the credit server 42 verifies that the received message includes the **correct key** in step 604. If the received message **does not include[s] the correct key**, the "NO" branch is followed to step 605 in which the point of presence 22 responds to a potentially fraudulent message. For example, the communication may be disconnected...." (emphasis added)

As set forth in the July 20, 2005 Amendment, as well as clearly disclosed in the cited portion of Roden, the reference teaches that a key is received and if, during verification, the key is determined to not be the correct key, disconnection can be effected. In other words, a key is received and it is verified in step 604 whether the key is correct or not correct (i.e., the cited teaching is a verification step). During verification, if the *correct* key is received, the credit server 42 generates a second time stamp; if the *wrong* key is received, the communication may be disconnected (col. 17, lines 35-39 and 49-52). There is simply no teaching or suggestion of a disconnection effected based upon **non-receipt** of the key, as recited in claim 1.

In the Attachment to the August 4, 2005 Advisory Action, the Examiner again maintains that the cited portion of Roden discloses the claimed feature. In addition, the Examiner maintains, "...this step 604 is to verify in the case that sometimes or occasionally or periodically the KEY may not be included with the received message. In this situation, the communication

will be disconnected, stopped, or logged out." Based on the Examiner's comments, the Examiner maintains that Roden does teach that in step 604, non-receipt of a KEY is contemplated and such occurrence will effect a disconnection. However, referring to the cited portion of Roden quoted above, the reference simply does not disclose that such a situation is contemplated or that disconnection will be performed upon the occurrence of such situation (i.e., the determination of whether a key is correct or incorrect $\neq$ the determination of whether a key is received at all). The Examiner appears to be reading features into Roden that are neither taught nor suggested.

In summary, Appellant submits that the verification of whether a received key is the correct key is not analogous to determining whether a key was received in order to effect disconnection. Thus, Appellant submits that Roden fails to teach or suggest the claimed feature of **executing a logout** when a second user processor in a receiver terminal **does not receive** a periodically distributed encryption key.

In view of the above, Appellant submits that Roden fails to cure the deficient teachings of Mittra, and thus, claim 1 is patentable over the cited references.

2. Claims 2, 3, 6 and 10

Since claims 2, 3, 6 and 10 are dependent upon claim 1, Appellant submits that such claims are patentable at least by virtue of their dependency.

3. Claims 7-9

Since claims 7-9 contain features that are analogous to the features of claim 1 discussed above, Appellant submits that claims 7-9 are patentable for at least analogous reasons as claim 1.

4. Claim 11

Since claim 11 is dependent upon claim 7, Appellant submits that such claim is patentable at least by virtue of its dependency.

B. Rejection of claims 1, 4 and 7-11 under 35 U.S.C. § 103(a) in view of Wesley and Roden

1. Claims 1 and 7-9

Claims 1 and 7-9 recite that a logout is executed when a receiver terminal or second user processor does not receive a periodically distributed encryption key.

The Examiner acknowledges that Wesley fails to disclose the above feature, but contends that Roden does (pg. 9 of April 20, 2005 Office Action). For analogous reasons as set forth above, Appellant submits that Roden fails to teach or suggest the claimed feature and therefore fails to cure the deficient teachings of Wesley.

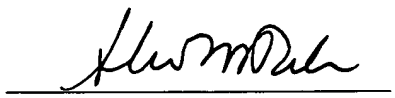
2. Claims 4, 10 and 11

Since claims 4, 10 and 11 are dependent upon one of claims 1 or 7, Appellant submits that such claims are patentable at least by virtue of their dependency.

Unless a check is submitted herewith for the fee required under 37 C.F.R. §41.37(a) and 1.17(c), please charge said fee to Deposit Account No. 19-4880.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,



Allison M. Tulino
Registration No. 48,294

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: December 20, 2005

CLAIMS APPENDIX

CLAIMS 1-4 and 6-11 ON APPEAL:

1. (rejected) A multicast system comprising:

a sender terminal for transmitting multicast data;

a receiver terminal for receiving multicast data;

an authentication server processor for managing the sender terminal and the receiver terminal;

a first user processor provided in the sender terminal for transmitting a login requirement to the authentication server processor; and

a second user processor provided in the receiver terminal for transmitting a login requirement to the authentication server processor,

wherein the authentication server processor executes a logout when the second user processor in the receiver terminal does not receive a periodically distributed encryption key which is periodically generated by the authentication server processor and distributed to the receiver terminal.

2. (rejected) A multicast system according to claim 1, wherein the sender terminal encrypts multicast data and transmits encrypted multicast data to the receiver terminal when the first user processor transmits the login requirement to the authentication server processor and when the authentication server processor permits login.

3. (rejected) A multicast system according to claim 1, wherein the receiver terminal registered in the authentication server processor decrypts encrypted multicast data using an encryption key distributed from the authentication server processor and receives decrypted multicast data in an application provided in the receiver terminal when the second user processor transmits the login requirement to the authentication server processor and when the authentication server processor permits login.

4. (rejected) A multicast system according to claim 1, wherein a receiver terminal, other than the receiver terminal registered in the authentication server processor, is rejected an encryption key distribution from the authentication server processor when the second user processor transmits the login requirement to the authentication server processor and when the authentication server processor rejects the login requirement.

Claim 5 (canceled)

6. (rejected) A multicast system according to claim 1, wherein the second user processor transmits a logout requirement to the authentication server processor and the authentication server processor terminates user management when multicast data communication is terminated in an application in the receiver terminal.

7. (rejected) An authentication server terminal comprising:

an authentication server processor;

a first receiving section for receiving a login requirement transmitted from a first user processor provided in a sender terminal which transmits multicast data;

a second receiving section for receiving a login requirement transmitted from a second user processor provided in a receiver terminal which receives multicast data; and

a user registration information section for registering user's individual information, wherein the user uses the sender terminal,

the sender terminal which is permitted login by the authentication server processor encrypts multicast data and transmits encrypted multicast data, and

the receiver terminal, which is registered as a user in the user registration information section by the authentication server processor, is permitted login and receives multicast data,

wherein the authentication server processor executes a logout when the second user processor in the receiver terminal does not receive a periodically distributed encryption key which is periodically generated by the authentication server processor and distributed to the receiver terminal.

8. (rejected) A multicast receiver terminal management method comprising the steps of:

registering a user's individual information transmitted from a sender terminal;

receiving a login requirement transmitted from the sender terminal which transmits multicast data;

managing the sender terminal which is permitted login so as to encrypt multicast data and to transmit encrypted multicast data;

receiving a login requirement transmitted from a receiver terminal which receives multicast data;

managing the receiver terminal which is registered as a user in a user registration information section by an authentication server processor, so as to be permitted login and to receive multicast data; and

executing a logout when the receiver terminal does not receive a periodically distributed encryption key which is periodically generated and distributed to the receiver terminal.

9. (rejected) A storage medium which is readable by a computer, for storing a multicast receiver terminal management method program for conducting multicast data communication in a computer, the multicast receiver terminal management method program comprising the steps of:

a registration step in which a user's individual information is registered, wherein the user uses a sender terminal;

a receiving step in which a login requirement, transmitted from the sender terminal which transmits multicast data, is received;

a managing step in which the sender terminal, which is permitted login, is managed so as to encrypt multicast data and to transmit encrypted multicast data;

a receiving step in which a login requirement, transmitted from the sender terminal which receives multicast data, is received;

a managing step in which a receiver terminal, which is registered as a user in a user registration information section by an authentication server processor, is managed so as to be permitted to login and to receive multicast data; and

wherein the authentication server processor executes a logout when the receiver terminal does not receive a periodically distributed encryption key which is periodically generated by the authentication server processor and distributed to the receiver terminal.

10. (rejected) The multicast system according to claim 1, wherein the login requirement of the first user processor and the second user processor is encrypted.

11. (rejected) The authentication server terminal according to claim 7, wherein the login requirement of the first user processor and the second user processor is encrypted.

EVIDENCE APPENDIX:

NONE

RELATED PROCEEDINGS APPENDIX

NONE